DTE_SECURITY: HERRAMIENTA PARA LA DISTRIBUCIÓN SEGURA Y LIMITADA DE DOCUMENTOS ELECTRÓNICOS

Fco Javier Molina[1], Alberto J. Molina[1], A. Ariel Gómez[1]. Julio Pérez[2]
[1]Departamento de Tecnología Electrónica. Escuela Universitaria Politécnica. Universidad de Sevilla, 41011-Sevilla
[2]EGMASA. Isla de la Cartuja. 41092-Sevilla

DTE_SECURITY es una herramienta diseñada específicamente para distribuir de forma segura y limitada libros, apuntes y manuales, generados en cualquier procesador de textos. En realidad, se trata de un plug-in que se inserta y amplía las funciones de las herramientas de edición electrónica de ADOBE: ACROBAT y ACROREAD. El objetivo que se persigue es aumentar la confianza de los autores en la publicación electrónica, mejorando su seguridad y ampliando las funciones que restringen el acceso a los mismos (consulta limitada, fechas de caducidad, redes de trabajo, usuarios registrados, ...)

1. El comercio de libros y documentos electrónicos.

El comercio de los libros electrónicos es una actividad relativamente reciente, cuya aparición se debe principalmente a dos factores: la popularización de los ordenadores personales, y la expansión de INTERNET como medio de distribución barato, abierto y directo [1]. Los bajos costes finales de las ediciones electrónicas han favorecido la aparición de pequeñas editoriales que compiten dentro de la red con productores más clásicos como Universidades y grandes editoriales. Todos ven en la venta directa a través de internet una nueva forma de negocio. Tanto la distribución como la producción son más económicas en formato electrónico, y por ello, se abre la posibilidad de realizar ediciones de baja tirada, es decir, en las que se esperan vender o distribuir pocos ejemplares, o más apropiadamente, pocas copias del documento. De hecho, pequeñas editoriales, o incluso el propio autor, pueden venderlos o distribuirlos directamente [2].

2. Seguridad en los documentos electrónicos.

La principal desventaja de la publicación electrónica es la desconfianza que existe sobre su seguridad. No falta razón a quienes piensan que un medio tan flexible se presta muy bien a la piratería. Estudios realizados en todo el mundo por empresas del sector han determinado la existencia de unos 7.000 títulos piratas que circulan en formato electrónico. Sin embargo, la inmensa mayoría de estos casos corresponde a publicaciones que no disponen de versiones electrónicas originales, sino que han sido escaneadas a partir de su formato impreso. Existen casos de violación (*cracks*) de documentos electrónicos, pero son mínimos. Los mecanismos de seguridad incrustados en ellos no son invulnerables, pero su complejidad es suficiente para obligar a un gran esfuerzo de piratería.

Los sistemas de seguridad existentes en el mundo de la publicación electrónica tienen en común el objetivo principal de impedir la alteración del contenido del documento, como forma de garantizar la integridad y la autoría del texto. Además, suelen ofrecer un sistema de contraseñas más o menos complejo con el que limitar el acceso al mismo, y un almacenamiento cifrado (encriptado), que asegure la inviolabilidad de la información contenida en el fichero.

3. Formatos electrónicos y herramientas comerciales.

En el mercado existen multitud de formatos electrónicos para documentos: Postcript, PDF, XML, LIT, EVY....[3] y un número mucho mayor de herramientas que generan libros electrónicos (*e-books)*. Los formatos más utilizados son el **PDF** y el **Postcript**, aunque en la actualidad el gigante Microsoft ha desarrollado uno propio: el **LIT**, fácilmente generable desde el popular WORD). En este momento, sin embargo, la mayor parte de las herramientas de generación emplean el PDF, y de todas ellas, las más popular es ***ACROBAT*** desarrollada por *ADOBE*, creador del formato. ADOBE ofrece un paquete de programas que permite la transformación de cualquier formato al estándar PDF. ACROBAT añade a estos ficheros muchas otras características, entre las que destacamos:

- **Seguridad**: contraseñas, encriptación, firmas digitales, ...
- **Vínculos**: dentro del documento, a direcciones WEB, de correo, ...
- **Anotaciones**, **incrustación de objetos** (WAVE, AVIS, ...)

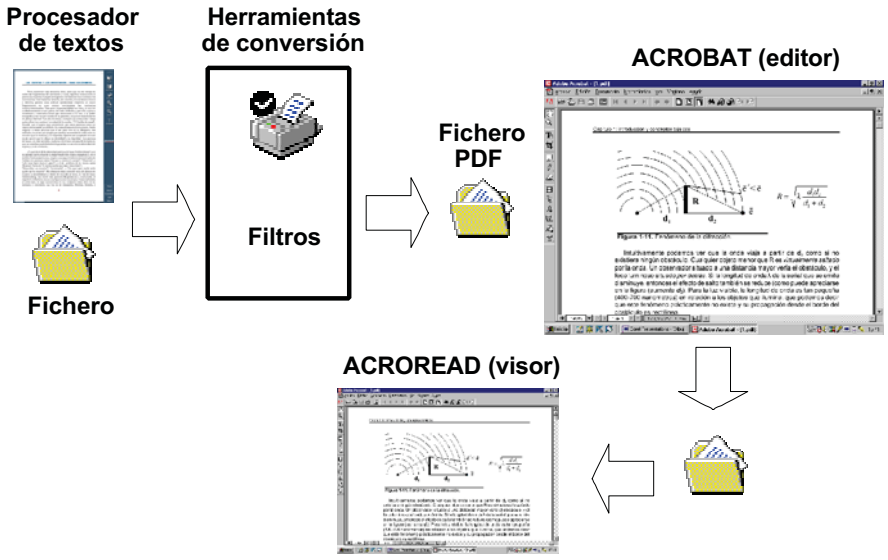

Figura 1. Generación y visualización de ficheros PDF con ADOBE.

Si se desea, estos programas disponen de un sistema de gestión de seguridad bastante sofisticado, que incluye las siguientes opciones:

- Texto y gráficos no editables.
- Contraseñas para abrir el documento o para cambiar las opciones de seguridad
- Información encriptada en el fichero (sólo cuando se establecen contraseñas)
- Impedir la impresión, o la selección de texto y gráficos.
- Firmas digitales (el documento se asocia al autor, cualquier cambio se añade, se registra y se firma sin modificar el anterior).

4. Características de *DTE_Security*

DTE_Security es un *plug-in* que añade limitaciones al acceso y uso del documento electrónico, y lo almacena siempre encriptado con una clave de 40 bits. Las funciones que el *plug-in* suma a las de ACROBAT son las siguientes:

- **Nueva gestón de contraseñas/encriptación**. Las opciones de seguridad que incorpora *DTE_Security* permiten añadir contraseñas para abrir el archivo y para modificar las condiciones de seguridad preestablecidas. El usuario común del visor (ACROREAD) no puede modificar los parámetros de seguridad incrustados en el documento. La contraseña de seguridad protege de cambios en el caso de que se utilice el editor ACROBAT. En cualquier caso, la información que se genera en el fichero: texto, estructura del documento, datos de seguridad, etc., se almacena encriptada. ACROBAT permite utilizar su mecanismo interno de cifrado, o que el usuario emplee uno propio. En esta versión del plugin hemos optado por utilizar el algoritmo interno. El proceso se realiza mediante un sistema de doble clave con el que se encripta por separado cada uno de los objetos contenidos en el documento (cadenas, anotaciones, estructura de las páginas, estructura del documento, ...).

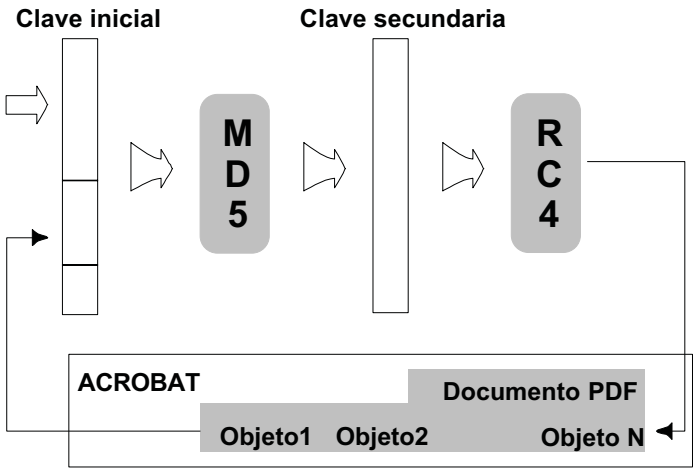

Figura 2. Proceso de encriptación con ACROBAT.

- **Limitar el uso temporal del documento**: por calendario o por tiempo de consulta. El autor puede seleccionar una fecha límite para fijar la disponibilidad o validez temporal del documento (p.e. cursos académicos), o bien puede definir un tiempo máximo de consulta transcurrido el cual el documento no puede abrirse. De este modo, se ofrece al lector la posibilidad de comprobar su interés por el documento.

- **Restringir el documento a un único usuario o a un grupo de trabajo**: *identificando el computador*, *detectando el número de serie del CD-ROM* donde se distribuye el documento, o *identificando una red local (LAN)*.

  La detección de un CD-ROM se emplea para asociar el fichero del documento a un CD, de modo que éste actúa como un disco llave. Esta utilidad es interesante en la distribución mediante CD-ROM de pequeñas tiradas. Los grabadores identifican los CD con números diferentes, lo que permite *incrustar*, o ligar el documento a un CD-ROM concreto.

La limitación a una red local permite la creación de grupos de trabajo con acceso al documento, y que éste circule libremente por la red, con la seguridad de que otros usuarios no podrán utilizarlo. Al abrirse el documento, el *plug-in* busca dentro de la red local un directorio compartido con o sin contraseña (recomendamos esta segunda opción). El documento sólo se abre si logra conectarse a dicho recurso. Este método es además independiente del protocolo de red (IP, NETBUI, NOVELL, etc).

5. Futuras opciones.

En el momento de presentar este documento, se encuentran bajo desarrollo dos nuevas opciones. Reducir la calidad de impresión y visualización en pantalla, y obtener los permisos desde un servidor de licencias via WEB.

El objetivo de limitar la calidad de la impresión y la visualización es reducir las prestaciones de los paquetes de reconocimiento de caracteres OCR. Bien mediante escáner o mediante una impresión de pantalla, el usuario puede obtener imágenes electrónicas de las páginas del documento. Estas características permitirán degradar de forma programada y seleccionable la presentación en pantalla y las copias impresas. Se están evaluando tres métodos alternativos: la utilización de fuentes no convencionales (con líneas o trazos dobles en diferentes colores), la incrustación de marcas de agua de pequeño tamaño, y la degradación tanto de las fuentes como del documento mediante ruido impulsivo.

La opción de conectar a un servidor de licencias abrirá un universo nuevo de posibilidades. Se podrán ofrecer permisos o licencias de campo a organismos o sociedades con grandes redes, así como a usuarios individuales conectados a INTERNET. Cualquiera de las opciones ya descritas en cuanto a seguridad, límite temporal, etc, pueden gestionarse ON-LINE desde este servidor. También será posible analizar desde el servidor el uso del documento por diferentes lectores, establecer perfiles de usuario, elaborar estadísticas, etc...

6. Conclusiones

El gestor de seguridad *DTE_Security* es una herramienta diseñada para aumentar la confianza de los autores en la publicación electrónica, y estimular por ende la producción de libros, manuales, apuntes o cualquier clase de documento. *DTE_Security* ofrece a la vez seguridad en el contenido y flexibilidad para seleccionar quiénes y de qué forma pueden utilizar el documento.

Referencias

[1] Peek-RP. *Where is publishing going? A perspective on change.* JASIS. vol.45, no.10; Dec. 1994; p.730-6

[2] Anne Christie. *Virtual universities and the publishing revolution: a publisher's viewpoint* Library Hi Tech, Volume 17, Number 1 (1999)

[3] Sanchez-EF; Morales-IF. *Web journal publishing: a general perspective* El-Profesional-de-la-Informacion. vol.9, no.3; March 2000; p.4-12